

Points on singular Frobenius nonclassical curves

Herivelto Borges

ICMC, Universidade de São Paulo, São Carlos, Brazil

Masaaki Homma

Department of Mathematics and Physics, Kanagawa University, Hiratsuka 259-1293, Japan

November 3, 2015

Abstract

In 1990, Hefez and Voloch proved that the number of \mathbb{F}_q -rational points on a nonsingular plane q -Frobenius nonclassical curve of degree d is $N = d(q - d + 2)$. We address these curves in the singular setting. In particular, we prove that $d(q - d + 2)$ is a lower bound on the number of \mathbb{F}_q -rational points on such curves of degree d .

Keywords: Algebraic curve, Frobenius nonclassical curve, Finite Field.

2010 Mathematics Subject Classification: Primary 14H45; Secondary 14Hxx.

1 Introduction

Let p be a prime number and \mathbb{F}_q be the field with $q = p^s$ elements, for some integer $s \geq 1$. An irreducible plane curve \mathcal{C} , defined over \mathbb{F}_q , is called q -Frobenius nonclassical if the q -Frobenius map takes each simple point $P \in \mathcal{C}$ to the tangent line to \mathcal{C} at P . In this case, there is an exponent h with $p \leq p^h \leq d$ so that the intersection multiplicity $i(\mathcal{C}, T_P(\mathcal{C}); P)$ of \mathcal{C} and the tangent line $T_P(\mathcal{C})$ at a simple point $P \in \mathcal{C}$ is at least p^h , and actually $i(\mathcal{C}, T_P(\mathcal{C}); P) = p^h$ holds for a general point $P \in \mathcal{C}$.

For convenience,

$$\nu = \begin{cases} p^h & \text{if } \mathcal{C} \text{ is } q\text{-Frobenius nonclassical} \\ 1 & \text{if } \mathcal{C} \text{ is } q\text{-Frobenius classical} \end{cases} \quad (1.1)$$

is called the q -Frobenius order of \mathcal{C} .

Frobenius nonclassical curves were introduced in the work of Stöhr and Voloch [7], and one reason for highlighting this special class of curves comes from the following result (see [7, Theorem 2.3]).

Theorem 1.1 (Stöhr-Voloch). *Let \mathcal{C} be an irreducible plane curve of degree d and genus g defined over*

\mathbb{F}_q . If $\mathcal{C}(\mathbb{F}_q)$ denotes the set of \mathbb{F}_q -rational points on \mathcal{C} , then

$$\#\mathcal{C}(\mathbb{F}_q) \leq \frac{\nu(2g-2) + (q+2)d}{2}. \quad (1.2)$$

Note that by \mathbb{F}_q -rational points on \mathcal{C} , we mean the \mathbb{F}_q -rational points on the nonsingular model of \mathcal{C} . Based on Theorem 1.1, Frobenius nonclassicality can be considered as an obstruction to use the nicer upper bound given by inequality (1.2) with $\nu = 1$. That is a clear reason why one should try to understand such curves better. At the same time, investigating Frobenius nonclassical curves is a way of searching for curves with many points. For instance, the Hermitian curve

$$x^{q+1} + y^{q+1} = 1,$$

over \mathbb{F}_{q^2} , and the Deligne-Lusztig-Suzuki curve over \mathbb{F}_q :

$$y^q - y = x^{q_0}(x^q - x),$$

where $q_0 = 2^s$, $s \geq 1$, and $q = 2q_0^2$, which are well known examples of curves with many points, are Frobenius non-classical.

With regard to the number of rational points, a somewhat surprising fact was proved by Hefez and Voloch in the case of nonsingular curves (see [3]).

Theorem 1.2 (Hefez-Voloch). *Let \mathcal{X} be a nonsingular q -Frobenius nonclassical plane curve of degree d defined over \mathbb{F}_q . If $\mathcal{X}(\mathbb{F}_q)$ denotes the set of \mathbb{F}_q -rational points on \mathcal{X} , then*

$$\#\mathcal{X}(\mathbb{F}_q) = d(q - d + 2). \quad (1.3)$$

Let us recall that if \mathcal{X} is a nonsingular q -Frobenius nonclassical plane curve of degree d , and $\nu > 2$ is its q -Frobenius order defined in (1.1), then (see [5, Theorem 8.77])

$$\sqrt{q} + 1 \leq d \leq \frac{q-1}{\nu-1}. \quad (1.4)$$

Now note that if $\nu > 3$ and d is within the range given by (1.4), then

$$d(q - d + 2) > \frac{d(q + d - 1)}{2}, \quad (1.5)$$

where the number on the right hand side of (1.5) is the bound given by Theorem 1.1 for the case $\nu = 1$. In other words, (1.3) tells us that nonsingular Frobenius nonclassical curves of degree d usually have many rational points in comparison with the Frobenius classical ones of the same degree. In this paper, we show that this statement could be applied more broadly if we were to drop the exclusivity on nonsingularity.

More precisely, we prove the following:

Theorem 1.3. *Let \mathcal{C} be a q -Frobenius nonclassical curve of degree d and genus g . If M_q^S is the number of simple points of \mathcal{C} in $PG(2, q)$, then*

$$M_q^S \geq d(q - d + 2) + 2(g^* - g) + \sum_{P \in \text{Sing}(\mathbb{F}_q)} m_P(m_P - 2), \quad (1.6)$$

where m_P are the multiplicities of the singular points $P \in \text{Sing}(\mathbb{F}_q) \subseteq PG(2, q)$ of \mathcal{C} , and

$$g^* := \frac{(d-1)(d-2)}{2} - \sum_{P \in \text{Sing}(\mathbb{F}_q)} \frac{1}{2} m_P(m_P - 1)$$

is its \mathbb{F}_q -virtual genus. Moreover, equality holds in (1.6) if and only if all branches of \mathcal{C} are linear.

Note that the bound (1.6) does not depend on the Frobenius order ν . A very interesting consequence of Theorem 1.3 is the following:

Corollary 1.4. *Let \mathcal{C} be a q -Frobenius nonclassical curve of degree d . If M_q is the number of points of \mathcal{C} in $PG(2, q)$, then*

$$M_q \geq d(q - d + 2), \quad (1.7)$$

and equality holds if and only if \mathcal{C} is nonsingular.

2 Preliminaries

Let us begin by briefly recalling the notions of classicality and q -Frobenius classicality for plane curves. For a more general discussion, including the notion and properties of branches, we refer to [5] and [4].

Let $\mathcal{C} \subset \mathbb{P}^2$ be an irreducible algebraic curve of degree d and genus g . The numbers $0 = \epsilon_0 < \epsilon_1 = 1 < \epsilon_2$ represent all possible intersection multiplicities of \mathcal{C} with lines of \mathbb{P}^2 at a generic point of \mathcal{C} . Such a sequence is called the order sequence of \mathcal{C} , and it can be characterized as the smallest sequence (in lexicographic order) such that $\det(D_\zeta^{\epsilon_i} x_j) \neq 0$, where D_ζ^k denotes the k th Hasse derivative with respect to a separating variable ζ , and x_0, x_1, x_2 are the coordinate functions on $\mathcal{C} \subset \mathbb{P}^2$. The curve \mathcal{C} is called classical if $\epsilon_2 = 2$.

If \mathcal{C} is defined over a finite field \mathbb{F}_q , then there is a smallest integer $\nu \in \{1, \epsilon_2\}$ such that

$$\begin{pmatrix} x_0^q & x_1^q & x_2^q \\ x_0 & x_1 & x_2 \\ D_\zeta^\nu x_0 & D_\zeta^\nu x_1 & D_\zeta^\nu x_2 \end{pmatrix} \neq 0 \quad (2.1)$$

The number ν is called the q -Frobenius order of \mathcal{C} , and such a curve is called q -Frobenius classical if $\nu = 1$.

Associated to the curve \mathcal{C} , there exist two distinguished divisors R and S , which play an important role in estimating the number of \mathbb{F}_q -rational points of \mathcal{C} . When the curve is Frobenius nonclassical, some valuable information can be obtained by comparing the multiplicities $v_P(R)$ and $v_P(S)$ for the points $P \in \mathcal{C}$. In general, computing these multiplicities is tantamount to studying some functions in $\overline{\mathbb{F}}_q(x, y)$ given by Wronskian determinants such as $\det(D_\zeta^{\epsilon_i} x_j)$ and (2.1). This idea was first exploited by Hefez and Voloch, in their investigation of the nonsingular case [3]. As noted by Hirschfeld and Korchmáros in [4], this idea can be useful in the singular case as well.

Let $\overline{\mathbb{F}}_q(\mathcal{C}) := \overline{\mathbb{F}}_q(x, y)$ be the function field of an irreducible curve $\mathcal{C} : f(x, y) = 0$. Recall that for any given place \mathcal{P} of $\overline{\mathbb{F}}_q(\mathcal{C})$ and a local parameter t at \mathcal{P} , one can associate a (primitive) branch γ in special affine coordinates:

$$x(t) = a + a_1 t^{j_1} + \cdots, \quad y(t) = b + b_1 t^s + \cdots,$$

where $s \geq j_1$. The point $(a, b) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ is called the center of the branch γ .

The branch γ is called linear if $j_1 = 1$. If $p \nmid j_1$ (resp. $p \mid j_1$) then the branch is called tame (resp. wild). Obviously, linear branches are tame.

When the curve $\mathcal{C} : f(x, y) = 0$ is defined over \mathbb{F}_q , then $\mathcal{C}(\mathbb{F}_q)$ will denote the set of places of degree one in the function field $\mathbb{F}_q(\mathcal{C})$. Considering the projective closure $F(x, y, z) = 0$ of \mathcal{C} , we define the following numbers, which are clearly related to $\#\mathcal{C}(\mathbb{F}_q)$:

Definition 2.1. (i) $M_q^S =$ number of smooth points of $F(x, y, z) = 0$ in $PG(2, q)$.

(ii) $M_q =$ number of points of $F(x, y, z) = 0$ in $PG(2, q)$.

(iii) $B_q =$ number of branches of \mathcal{C} centered at a point in $PG(2, q)$.

Note that

$$M_q^S \leq M_q \leq B_q \text{ and } M_q^S \leq \#\mathcal{C}(\mathbb{F}_q) \leq B_q. \quad (2.2)$$

Hereafter, \mathcal{C} will denote an irreducible plane curve of degree d and genus g defined over \mathbb{F}_q . A relevant step to prove our main result is based on the following:

Theorem 2.2 (Hirschfeld-Korchmáros). *Assume that \mathcal{C} has only tame branches. If \mathcal{C} is a nonclassical and q -Frobenius nonclassical curve, then*

$$B_q \geq (q-1)d - (2g-2),$$

and equality holds if and only if every singular branch of \mathcal{C} is centered at a point of $PG(2, q)$.

The next lemma extends Hirschfeld-Korchmáros' result, and our proof is built on theirs. In particular, all the definitions and notations, explained in detail in [4], will be borrowed.

Lemma 2.3. *If \mathcal{C} is q -Frobenius nonclassical, then there exist at least $(q-1)d - (2g-2)$ tame branches centered at a point of $PG(2, q)$. In particular,*

$$B_q \geq (q-1)d - (2g-2). \quad (2.3)$$

Moreover, if every branch centered at a point of $PG(2, q)$ is tame, then (2.3) is an equality if and only if all the remaining branches are linear.

Proof. We closely follow the notation used in [4].

Set

$$\det(D_\zeta^{(\epsilon_i)} x_j) = \begin{vmatrix} D_\zeta^{(1)} x & D_\zeta^{(1)} y \\ D_\zeta^{(p^m)} x & D_\zeta^{(p^m)} y \end{vmatrix} \quad \text{and} \quad \det(D_\zeta^{(\nu_i)} x_j) = \begin{vmatrix} x^q - x & y^q - y \\ D_\zeta^{(p^m)} x & D_\zeta^{(p^m)} y \end{vmatrix}$$

The q -Frobenius nonclassicality of \mathcal{C} gives

$$\begin{vmatrix} x^q - x & y^q - y \\ D_\zeta^{(1)} x & D_\zeta^{(1)} y \end{vmatrix} = 0, \quad (2.4)$$

and then establishes the relation

$$\det(D_\zeta^{(\nu_i)} x_j) \cdot D_\zeta^{(1)} x = \det(D_\zeta^{(\epsilon_i)} x_j) \cdot (x^q - x).$$

Therefore, for any place \mathcal{P} of $\overline{\mathbb{F}}_q(\mathcal{C})$,

$$v_{\mathcal{P}}(S) - v_{\mathcal{P}}(R) = \text{ord}_{\mathcal{P}}(x^q - x) - \text{ord}_{\mathcal{P}}(D_\zeta^{(1)} x). \quad (2.5)$$

Let γ be the (primitive) branch associated to the place \mathcal{P} , represented by

$$x(t) = a + a_1 t^{j_1} + \cdots, \quad y(t) = b + b_1 t^s + \cdots,$$

with $j_1 \leq s$. If γ is tame, i.e., $p \nmid j_1$, then it follows (see [4, proof of Theorem 1.4]) that

$$v_{\mathcal{P}}(S) - v_{\mathcal{P}}(R) = \begin{cases} 1, & \text{if } (a, b) \in \mathbb{F}_q \times \mathbb{F}_q; \\ -(j_1 - 1), & \text{otherwise.} \end{cases} \quad (2.6)$$

Now let us address the wild case, i.e., the case $p \mid j_1$. Note that if $D_\zeta^{(1)} x = 0$ then, from (2.4), we have $D_\zeta^{(1)} y = 0$, which contradicts the primitivity of γ . Hence, $\text{ord}_{\mathcal{P}}(D_\zeta^{(1)} x) = k > j_1 - 1$ and (2.5) yield

$$v_{\mathcal{P}}(S) - v_{\mathcal{P}}(R) = \begin{cases} -(k - j_1), & \text{if } a \in \mathbb{F}_q; \\ -k, & \text{otherwise.} \end{cases} \quad (2.7)$$

Therefore, (2.6) and (2.7) can be reduced to

$$v_{\mathcal{P}}(S) - v_{\mathcal{P}}(R) = \begin{cases} 1, & \text{if } \gamma \text{ is tame with center in } PG(2, q); \\ \leq 0, & \text{otherwise.} \end{cases}$$

Hence, since $\deg(S - R) = d(q - 1) - (2g - 2)$, we arrive at the desired lower bound for the number of tame branches centered at a point of $PG(2, q)$.

Now let us assume that every branch centered at a point of $PG(2, q)$ is tame. If $B_q = d(q - 1) - (2g - 2)$, then (2.6) implies that the remaining tame branches are linear. In addition, (2.7) implies that any wild branch can be considered as

$$x(t) = a + a_1 t^{j_1} + \cdots, \quad y(t) = b + b_1 t^s + \cdots,$$

with $2 \leq j_1 \leq s$, $\text{ord}_{\mathcal{P}}(D_{\zeta}^{(1)} x) = j_1$ and $a \in \mathbb{F}_q$. However, if this is the case, then from

$$\text{ord}_{\mathcal{P}}((x^q - x)(D_{\zeta}^{(1)} y)) = \text{ord}_{\mathcal{P}}((y^q - y)(D_{\zeta}^{(1)} x)),$$

we obtain

$$\text{ord}_{\mathcal{P}}(y^q - y) = \text{ord}_{\mathcal{P}}(D_{\zeta}^{(1)} y) \geq s - 1 \geq 1,$$

i.e., $b \in \mathbb{F}_q$. Thus, by hypothesis, such branch must be tame, and then the assertion follows. The converse follows immediately from the fact that linear branches are automatically tame. □

3 The result

The aim of this section is to prove Theorem 1.3 and some of its relevant corollaries.

Proof of Theorem 1.3. Note that from Lemma 2.3 and the definition of B_q , we have

$$(q - 1)d - (2g - 2) \leq B_q \leq \sum_{P \in PG(2, q)} m_P. \quad (3.1)$$

Let M_q^S be the number of smooth \mathbb{F}_q -points on \mathcal{C} , and set $g^* = \frac{(d-1)(d-2)}{2} - \sum_{P \in \text{Sing}(\mathbb{F}_q)} \frac{1}{2} m_P (m_P - 1)$.

Then

$$\begin{aligned}
M_q^S &= \sum_{P \in PG(2,q)} m_P - \sum_{P \in Sing(\mathbb{F}_q)} m_P \\
&= \sum_{P \in PG(2,q)} m_P - \sum_{P \in Sing(\mathbb{F}_q)} m_P(m_P - 1) + \sum_{P \in Sing(\mathbb{F}_q)} m_P(m_P - 2) \\
&= \sum_{P \in PG(2,q)} m_P + (2g^* - 2) - (d^2 - 3d) + \sum_{P \in Sing(\mathbb{F}_q)} m_P(m_P - 2) \\
&= \sum_{P \in PG(2,q)} m_P - \left((q-1)d - (2g-2) \right) + d(q-d+2) + 2(g^* - g) + \sum_{P \in Sing(\mathbb{F}_q)} m_P(m_P - 2).
\end{aligned}$$

Since (3.1) gives $\sum_{P \in PG(2,q)} m_P - \left((q-1)d - (2g-2) \right) \geq 0$, it follows that

$$M_q^S \geq d(q-d+2) + 2(g^* - g) + \sum_{P \in Sing(\mathbb{F}_q)} m_P(m_P - 2). \quad (3.2)$$

Now note that equality on the latter case is equivalent to equality on both sides of (3.1). Let us assume we have equality in (3.2). The condition $B_q = \sum_{P \in PG(2,q)} m_P$ means that all branches centered at a point of $PG(2,q)$ are linear and then tame. Using the additional equality $B_q = (q-1)d - (2g-2)$, Lemma 2.3 implies that all branches of \mathcal{C} are linear. Conversely, the linearity of all branches of \mathcal{C} immediately gives $B_q = \sum_{P \in PG(2,q)} m_P$ and, from Lemma 2.3, $B_q = (q-1)d - (2g-2)$. \square

Proof of Corollary 1.4. From (2.2) and (1.6), we clearly have $M_q \geq d(q-2+d)$. Let us assume that equality holds. Then (2.2) and (1.6) imply $M_q^S = M_q$ and $g = g^*$, respectively. The first equality means that all points \mathbb{F}_q -points of \mathcal{C} are smooth, and thus $g^* = (d-1)(d-2)/2$. The latter equality, in addition, gives $g = (d-1)(d-2)/2$. Therefore, \mathcal{C} is a smooth curve. Conversely, if \mathcal{C} is smooth then $M_q = B_q$, and Lemma 2.3 gives $B_q = (q-1)d - (2g-2)$. Since $g = (d-1)(d-2)/2$, the result follows. \square

The following additional consequences are also worth mentioning.

Corollary 3.1. *Let \mathcal{C} be a q -Frobenius nonclassical curve of degree d whose singularities are ordinary. If the singular points have their tangent lines defined over \mathbb{F}_q , then*

$$\#\mathcal{C}(\mathbb{F}_q) = d(q-d+2) + \sum_{P \in \mathcal{C}} m_P(m_P - 1).$$

Proof. Note that all singularities are ordinary and defined over \mathbb{F}_q . Thus $g^* = g$, and equality in (1.6) holds. That is,

$$M_q^S = d(q - d + 2) + \sum_{P \in \text{Sing}(\mathbb{F}_q)} m_P(m_P - 2).$$

On the other hand, since the tangent lines of the singular points are defined over \mathbb{F}_q , each such point P gives rise to exactly m_P \mathbb{F}_q -rational points of \mathcal{C} . Therefore

$$\#\mathcal{C}(\mathbb{F}_q) = M_q^S + \sum_{P \in \text{Sing}(\mathbb{F}_q)} m_P = d(q - d + 2) + \sum_{P \in \text{Sing}(\mathbb{F}_q)} m_P(m_P - 1),$$

which gives the result. □

Corollary 3.2. *Let \mathcal{C} be a q -Frobenius nonclassical curve of degree $d > 1$. Then*

$$d \geq \sqrt{q} + 1,$$

and equality holds if and only if \mathcal{C} is (\mathbb{F}_q -isomorphic to) the Hermitian curve.

Proof. By Theorem 1.3 and Hasse-Weil bound, we have

$$d(q - d + 2) \leq M_q^S \leq 1 + q + (d - 1)(d - 2)\sqrt{q}.$$

Since $d(q - d + 2) \leq 1 + q + (d - 1)(d - 2)\sqrt{q}$ if and only if $(d - 1)(\sqrt{q} + 1)(\sqrt{q} + 1 - d) \leq 0$, the inequality $d \geq \sqrt{q} + 1$ follows. The additional assertion follows from a well known characterization of the Hermitian curve (see e.g. [5, Theorem 10.47]). □

Corollary 3.3. *Let \mathcal{C} be a plane curve defined over \mathbb{F}_q of degree d , with $1 < d \leq \sqrt{q}$, and genus g . Then*

$$\#\mathcal{C}(\mathbb{F}_q) \leq \frac{(2g - 2) + (q + 2)d}{2}.$$

Proof. This follows directly from Corollary 3.2 and Theorem 1.1. □

4 Examples

One can find several examples of Frobenius nonclassical curves that illustrate the previous results (see [1] and [2]). Let us consider the particular curve

$$\mathcal{C} : x^4y^2 + x^2y^4 + x^4yz + xy^4z + x^4z^2 + x^2y^2z^2 + y^4z^2 + x^2z^4 + xyz^4 + y^2z^4 = 0 \quad (4.1)$$

over \mathbb{F}_4 . This curve has some remarkable properties (see [1] and [6]). One particular feature of \mathcal{C} is its 4-Frobenius nonclassicality. The set of singular points of \mathcal{C} is the whole of $PG(2, 2)$, and all such singularities are nodes whose tangent lines are defined over \mathbb{F}_4 . Therefore, Corollary 3.1 gives

$$\#\mathcal{C}(\mathbb{F}_4) = 6(4 - 6 + 2) + 7 \cdot 2 \cdot (2 - 1) = 14.$$

The next example illustrates how the choice of singular q -Frobenius nonclassical curves of degree d , over nonsingular ones of the same degree, can make a significant difference with respect to the number of rational points. Consider the curves

$$\mathcal{C}_1 : x^{13} = y^{13} + z^{13}$$

and

$$\mathcal{C}_2 : x^{13} = y^{13} + y^9 z^4 + y^3 z^{10} + y z^{12} + 2z^{13},$$

over \mathbb{F}_{27} . They are both 27-Frobenius nonclassical, and only \mathcal{C}_1 is smooth. One can check that $\#\mathcal{C}_1(\mathbb{F}_{27}) = 208$, whereas $\#\mathcal{C}_2(\mathbb{F}_{27}) = 280$, in addition to \mathcal{C}_2 being of smaller genus.

References

- [1] H. Borges, On multi-Frobenius non-classical plane curves. Arch. Math. 93(6) (2009) 541–553.
- [2] H. Borges, Frobenius nonclassical components of curves with separated variables, <http://arxiv.org/abs/1311.4438> (2013).
- [3] A. Hefez, J.F. Voloch, Frobenius nonclassical curves, Arch. Math. 54(1990) 263–273.
- [4] N. J.W.P. Hirschfeld, G. Korchmáros, On the number of solutions of an equation over a finite field, Bull. Lond. Math. Soc. 33 (2001) 16–24.
- [5] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic curves over finite fields*, Princeton University Press, Princeton and Oxford, 2008.
- [6] M. Homma, S. J. Kim, Sziklai’s conjecture on the number of points of a plane curve over a finite field III. Finite Fields and Their Applications 16(5) (2010) 315–319.
- [7] K.O. Stöhr, J.F. Voloch, Weierstrass points on curves over finite fields, Proc. London Math. Soc. 52(1986) 1–19.